TITLE:

量子暗号の原理 (符号と暗号の代数的数理)

AUTHOR(S):

内山, 智香子

CITATION:

内山, 智香子. 量子暗号の原理 (符号と暗号の代数的数理). 数理解析研究所講究録 2004, 1361: 139-142

ISSUE DATE:

2004-04

URL:

http://hdl.handle.net/2433/25266

RIGHT:

京都大学学術情報リポジトリ
KURENAI 紅
Kyoto University Research Information Repository

数理解析研究所講究録 1361 巻 2004 年 139-142

量子暗号の原理

山梨大学　大学院医学工学総合研究部　内山智香子
Chikako Uchiyama
Interdisciplinary Graduate School of Medicine and Engineering,
University of Yamanashi

平成16 年1 月30 日

概 要

インターネットが普及し、情報の安全性に対する要求が急速に高まってきている中、この要求に答えうるものの一つとして注目されているのが量子暗号である。本講では、量子暗号の原理について紹介する[1]。

1 はじめに

送信者 (Alice) と受信者 (Bob) が情報を安全に通信したい場合、最も古典的な暗号は、通信文の暗号化と復号化に同じ暗号鍵を用いる共通鍵暗号であった。この方法では、配布された暗号鍵を1回のみ使用 (One Time Pad) した場合の安全性が、Shannon によって証明されている [2]。しかし、送信者と受信者の間で共有される暗号鍵が秘匿されなければこの安全性を保証することはできない。量子暗号はこの欠点を克服するために提案されたものであり、正確には量子論的な暗号鍵の配布 (Quantum Key Distribution) を意味する。その真髄は、量子力学の原理を用いることによって、盗聴者の存在の有無を知ることができるような通信規約 (プロトコル) を作成することが可能となったことにある。

量子暗号で用いる量子力学の原理は、量子力学的な状態に対する「重ね合わせの原理」と呼ばれるものである。ここで量子力学的な状態の一例として、光の偏光状態をとりあげることにする。偏光状態にも色々な種類があるが、最も単純なものに直線偏光がある。これは、電磁波である光が伝播する際に、電場、磁場の振幅の変化方向 (偏

[1]詳細については、文献 [1] 及びその中に引用されている文献をご参照下さい。

光方向）が直線に限られているものである。どのような光でも偏光板を通せば、偏光板の偏光軸に平行な偏光方向を持つ直線偏光となる。例えば、斜め45度方向に偏光軸を傾けた偏光板に光を入射すれば、斜め方向の直線偏光が得られる。以下では、この偏光状態を$|\nearrow>$と表示することにする。次に、光の偏光状態を観測する手段について考える。これには、方解石の結晶を用いる。適当な方向に方解石の結晶を切り出すと、例えば、水平方向$|\leftrightarrow>$と垂直方向$|\updownarrow>$といった互いに直交した偏光状態を区別できるようになる。上述の斜め方向の直線偏光をこの方解石の結晶に入射すると光が2筋に分かれ、水平方向の偏光状態の光と垂直方向の偏光状態の光とが異なる場所から出力される。日常世界で用いる強度の光を入射したときには、2筋に分かれるように見えるが、光を極端に減衰して光子と呼ばれるエネルギーの粒1つだけが方解石の結晶に入射するようにすると、事情は異なってくる。というのも、光子はそれ以上分割することのできない、エネルギーの最小単位であるので、方解石の結晶に入射した後、2個のエネルギー粒子に分かれて出力するわけにいかないからである。実際には、エネルギー粒子は、ある確率で水平方向の偏光状態の光子となって出力されたり、垂直方向の偏光状態の光子となって出力されたりする。前述の斜め45度方向の偏光状態$|\nearrow>$を入射すると、$|\leftrightarrow>$と$|\updownarrow>$とが各々５０%の確率で出力されることになる[2]。この状況は、斜め45度方向の偏光状態$|\nearrow>$が水平方向$|\leftrightarrow>$と垂直方向$|\updownarrow>$の重ね合わせ状態になっていることを示している。そして、量子暗号はこの重ね合わせ状態の観測についての量子力学的な性質を最大限に利用している。量子状態である斜め方向の直線偏光状態にある光子を方解石によって観測すると、斜め方向の偏光状態は変化して水平方向か垂直方向かのどちらかの偏光状態の光子が得られることになる。量子暗号の基礎を築いたBennettとBrassardは、この原理を盗聴者検出のために利用できないかと考えた[3]。光の偏光状態に情報を載せ、伝送している間に盗聴者がその光を盗み取り、情報を読み出そうと方解石の結晶をかざした瞬間に光の偏光状態が変化してしまう。この変化を送受信者が知ることができれば、盗聴者の有無が判別できる、というわけである。次に彼らの考案したBB84プロトコルと呼ばれる通信規約を紹介する。

2　ＢＢ８４プロトコル

BennettとBrassardの考案したプロトコル[3]では、光子等の量子状態を送受信する量子通信路と、電話やインターネット等の盗聴されてもかまわない古典的通信路の2

[2]この方解石の結晶に水平方向$|\leftrightarrow>$または垂直方向$|\updownarrow>$の光子を入射した場合には、１００%の確率で確実に観測できる。また、方解石の結晶の方向を45度傾けると、今度は斜め45度方向$|\nearrow>$と斜め135度方向$|\nwarrow>$が１００%の確率で確実に観測できるようになる。

種類の通信路を用いる。実際の通信手順は以下のとおりである。

1. 送信者 (Alice) と受信者 (Bob) は、0と1がランダムに並んだ乱数列をそれぞれ用意する。

2. 送信者 (Alice) は、自分の用意した乱数列に従い、光子を送信する。このとき、それぞれのビット値に2種類の偏光状態を割り当て、これをランダムに選ぶことにする。例えば、ビット値1を送信したい場合には、垂直方向 $|\updownarrow>$ か、斜め135度方向の直線偏光 $|\nwarrow>$ のどちらかをランダムに選び、ビット値0を送信したい場合には、水平方向 $|\leftrightarrow>$ か斜め45度方向 $|\nearrow>$ をランダムに選ぶものとする。

3. 受信者 (Bob) は方解石の結晶を用い、送信者 (Alice) から送られてきた光子の偏光状態を観測する。その際に自分の用意した乱数列に従って、方解石の結晶の方向を変える。例えば乱数列のビット値が1であれば、垂直方向か水平方向の光子が出力される方向に方解石の結晶を向け、ビット値が0であれば斜め135度か45度方向の光子が出力される方向に方解石の結晶を向けるものとする。この観測によって、垂直方向 $|\updownarrow>$ か、斜め135度方向の直線偏光状態 $|\nwarrow>$ を得た場合には、ビット値1を、水平方向 $|\leftrightarrow>$ か斜め45度方向直線偏光状態 $|\nearrow>$ を得た場合にはビット値0を受信したものとする。

4. すべての光子の送受信が終わった段階で、受信者 (Bob) は古典的通信路を用いて、各々のビット値の受信の際に用いた方解石の結晶の方向のみを送信者 (Alice) に伝える。このとき、観測結果そのものは通信しない。

5. 受信者 (Bob) の報告をうけ、送信者 (Alice) は自分の送信した光子の偏光状態と方解石の方向が一致したビットの番号を伝える。受信者 (Bob) は、伝えられた番号のビットの観測値のみを残す。同時に、送信者 (Alice) は送信前に自分の作成した乱数列のうち、受信者 (Bob) に伝えたビット番号に対応したもののみを残す。

こうして、送信者 (Alice) は通信前に作成した乱数列、受信者 (Bob) は光子の観測によって得た乱数列のうち、一部のみが残されることになる。そして、この抽出された乱数列は、両者の間で一致したものとなる。第4段階の古典的通信路を用いたやりとりでは、観測結果そのものを通信せず、観測の方法のみをやりとりしているところが重要である。

3 まとめと今後の展望

本稿では、Bennett と Brassard が最初に発表したプロトコルについて紹介した。その後、Bennett は 1992 年にこのプロトコルの改良版 (B92 プロトコル) を発表した [4]。これは、偏光状態のかわりに、光子の位相に情報を載せるものである。量子通信路として最初に採用された光ファイバーは、光の偏光状態を長距離にわたって伝送することが困難であることが、この改良が必要だった理由のひとつと考えられる。BB84 プロトコルの提案以来 20 年経った今日では、量子暗号は実用化段階に入っている [5]。量子通信路としては、やはり光ファイバーが主流で、100km 程度までなら問題なくやりとりできる。さらに長距離伝送を可能にするために、自由空間 [6, 7] を用いる方法が提案されている。

参考文献

[1] 内山智香子:別冊 数理科学「量子力学の発展」 (サイエンス社, 2001), p.132; 科学,vo.67 (岩波書店,1997), p.928.

[2] C.E.Shannon: Bell Syst.Tech.J.,28(1949), p.656.

[3] C.H.Bennet and G.Brassard: Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Banalore, India (IEEE, New York, 1984), p.175.

[4] C.H.Bennet: Phys. Rev. Lett., 68 (1992), p.3121.

[5] http://enterprise.watch.impress.co.jp/cda/foreign/2003/11/10/488.html; 日本経済新聞 (2002 年 11 月 15 日 PP.15)

[6] W.T.Buttler, et.al.: Phys. Rev. Lett., 81 (1998) p.3283 ; ibid, 84 (2000), p.5652.

[7] R.H.Hughes, et.al.:New Journal of Physics, 4 (2002) 43.1; J. Mod. Opt.,47 (2000), p.549.